THE MULTIPLICATIVE GROUP OF ABSOLUTELY
ALGEBRAIC FIELDS IN CHARACTERISTIC \( p \)

STEPHEN J. TILLMAN

Let \( p \) be a fixed prime number, and \( k \) an algebraic extension of \( F = \mathbb{Z}/p\mathbb{Z} \). Let \( F_c \) be the algebraic closure of \( F \). It is well known that

\[
G(F_c/F) \approx \hat{\mathbb{Z}} \approx \prod_{\text{all primes } q} Z_q,
\]

where \( Z_q \) is the \( q \)-adic integers. Hence \( G(k/F) \) is isomorphic to a factor group of \( \hat{\mathbb{Z}} \), and is essentially described by a supernatural number,

\[
N = \prod_{\text{all primes } q} q^{r(q)}
\]

where \( r(q) \) is either finite or infinite, and \( q^{r(q)} \) is the degree of the maximal \( q \)-extension of \( F \) in \( k \).

We shall show that the multiplicative group of \( k, k^* \), is isomorphic to a subgroup of

\[
\mathbb{Q}/\mathbb{Z} \approx \sum_{\text{all primes } q} Z(q^{\infty}),
\]

where \( Z(q^{\infty}) \) is the \( q \)-primary part of \( \mathbb{Q}/\mathbb{Z} \). Thus \( k^* \) is also described by a supernatural number,

\[
M = \prod_{\text{all primes } q} q^{s(q)},
\]

where \( s(q) \) is either finite or infinite and \( q^{s(q)} \) is the "order" of the \( q \)-Sylow subgroup of \( k^* \).

We shall see that the \( s(q) \)'s are completely determined by the \( r(q) \)'s defined in (1). In particular we shall easily be able to see when \( k^* \) is \( q \)-divisible for any prime \( q \).

**Definition.** For any group \( G \), we say \( G \) has condition \( T \) if \( \forall a, b \in G, \exists \) a cyclic subgroup \( H \) of \( G \) such that \( a, b \in H \).

**Proposition.** Any group with condition \( T \) is isomorphic to a subgroup of either \( \mathbb{Q} \) or \( \mathbb{Q}/\mathbb{Z} \).

**Proof (The proof of this proposition is due to Professor Michael I. Rosen).** Suppose \( G \) is a group with condition \( T \). Then \( G \)

Received by the editors July 11, 1968.

601
is either a torsion group, or a torsion free group, for if \(a, b \in G\), such that \(a\) has finite order and \(b\) has infinite order, then there exists no cyclic subgroup containing both \(a\) and \(b\), contradicting the assumption that \(G\) has condition \(T\). We shall assume that \(G\) is a torsion group, and prove the proposition only in this case. \(G\) is an abelian torsion group, hence it is isomorphic to the direct sum of its primary parts \(G_q\). We will show that \(G_q\) is either cyclic or isomorphic to \(\mathbb{Z}(q^\infty)\). This is sufficient to prove our assertion since \(\mathbb{Z}(q^\infty)\) is the \(q\)-primary component of \(\mathbb{Q}/\mathbb{Z}\). Obviously if \(G_q\) is finite it must be cyclic. Suppose \(G_q\) is infinite, and let \(h_1, h_2, h_3, \ldots\) be a sequence of distinct elements of \(G_q\). Let \(H_r\) be the subgroup generated by \(h_1, \ldots, h_r\). \(H_r\) is a finite cyclic group. Consider the chain \(H_1 \subseteq H_2 \subseteq H_3 \subseteq \ldots\). This chain cannot break off. Let \(H = \bigcup_{i=1}^{\infty} H_i\). It is easily seen that \(H\) is isomorphic to \(\mathbb{Z}(q^\infty)\). Since \(\mathbb{Z}(q^\infty)\) is a divisible group, \(H\) is a direct summand of \(G_q\). If it were a proper direct summand, \(G_q\) would contain a subgroup isomorphic to \(\mathbb{Z}/q\mathbb{Z} \oplus \mathbb{Z}/q\mathbb{Z}\). This is impossible since \(\mathbb{Z}/q\mathbb{Z} \oplus \mathbb{Z}/q\mathbb{Z}\) does not have condition \(T\), and condition \(T\) is inherited by subgroups. Thus \(H = G_q\) and \(G_q \cong \mathbb{Z}(q^\infty)\). QED

Remark. \(k^*\) has condition \(T\), and is torsion; hence by the above proposition we can write

\[
(3) \quad k^* \cong \sum_{\text{all primes } q} G_q,
\]

where \(G_q \subseteq \mathbb{Z}(q^\infty)\). Note that for any prime \(q\), \(k^*\) is \(q\)-divisible if and only if \(G_q\) is isomorphic to either \((0)\) or \(\mathbb{Z}(q^\infty)\).

**Proposition 1.** \(G_p \cong (0)\).

**Proof.** Suppose not. Then \(k^*\) contains a nontrivial element of order \(p\). This element would satisfy \(f(x) = x^p - 1 = 0\) over \(k[x]\); but since the characteristic at \(k\) is \(p\), \(1\) is the only solution to \(f(x) = 0\). QED

**Definition.** For any prime \(q \neq p\) define \(l(q)\) as the smallest positive integer such that \(p^{l(q)} \equiv 1(q)\).

**Proposition 2.** For any prime \(q \neq p\), if \(l(q) \nmid N\), then \(G_q \cong (0)\).

**Proof.** If \(G_q \cong (0)\), then some finite subfield, \(E\), of \(k\) has a nontrivial \(q\)-Sylow subgroup of its multiplicative group. We shall show that this is impossible. Let \(E\) be any finite subfield of \(k\). Then for some \(n \in \mathbb{Z}\), \(E^*\) has \(p^n - 1\) elements, and \(l(q) \nmid n\), for if it did, it would certainly divide \(N\). Hence \(n = ul(q) + v,\ 0 < v < l(q)\). \(p^n - 1 = p^v(p^{u(l(q))} - 1) + (p^v - 1)\). But by the definition of \(l(q)\), \(p^{u(l(q))} \equiv 1(q)\), and \(p^v \equiv 1(q)\), hence \(p^n - 1 \equiv p^v - 1 \equiv 0(q)\), so \(q \nmid p^n - 1\), and \(E^*\) has no nonzero \(q\)-subgroup. QED
Remark. Notice that $F$ has an $l(q)$-extension in $k$ if and only if $l(q) \mid N$.

Proposition 3. Let $q \neq p$ be any prime, and assume $F$ has an $l(q)$-extension in $k$. Then $k^*$ is $q$-divisible if and only if the maximal $q$-extension of $F$ in $k$ is infinite i.e., $r(q) = \infty$.

Proof. Suppose the maximal $q$-extension of $F$ in $k$ is infinite. Since we are assuming $F$ has an $l(q)$-extension in $k$, there exists a finite subfield $E$ such that $E^*$ has $p^n - 1$ elements and $n = l(q)m$. We have
\[
 p^n - 1 = (p^{l(q)} - 1)(p^{l(q)}(m-1) + p^{l(q)}(m-2) + \cdots + p^{l(q)} + 1).
\]
But by definition $p^{l(q)} = 1(q)$ hence $q \mid p^n - 1$, so $G_q \neq (0)$ (defined in equation (3)). Thus we must show $G_q \cong Z(q^n)$. Since we are assuming $r(q) = \infty$, it suffices to show that $q$-extensions have strictly increasing $q$-Sylow subgroups of their multiplicative groups. We must show that if
\[
 \alpha(n) > \alpha(n-1). \quad (\text{Equation (4) defines } \alpha(n).)
\]
then $\alpha(n) > \alpha(n-1)$. (Equation (4) defines $\alpha(n)$.)
\[
 p^{l(q)}q^n - 1 = (p^{l(q)}q^{n-1} - 1)(p^{l(q)}q^{n-2}(q-1) + p^{l(q)}q^{n-2}(q-2) + \cdots + 1)
 = q^{\alpha(n-1)}l_{n-1}(p^{l(q)}q^{n-1}(q-1) + \cdots + 1),
\]
so $\alpha(n) > \alpha(n-1)$ because $(p^{l(q)}q^{n-1}(q-1) + \cdots + 1)$ has $q$ terms, each congruent to $1$ mod $q$, hence is divisible by $q$.

Now suppose the maximal $q$-extension of $F$ in $k$ is finite. We saw in the proof of the first part of this proposition that the assumption $l(q) \mid N$ implies $G_q \neq (0)$. Hence if $k^*$ were $q$-divisible, we could find a finite subfield $E$ of $k$ such that the $q$-Sylow subgroup of $E^*$ has more than $q^{\alpha(r(q))}$ elements. Suppose $E$ is any such finite subfield. There is no loss of generality in assuming that $E$ contains an $l(q)$-extension and a maximal $q$-extension of $F$ in $k$. Thus $E^*$ has $p^{l(q)q^{r(q)m}} - 1$ elements, where $q \mid m$. But
\[
 p^{l(q)q^{r(q)m}} - 1 = (p^{l(q)q^{r(q)}} - 1)(p^{l(q)q^{r(q)}}(m-1) + \cdots + 1)
 = q^{\alpha(r(q))}t_{r(q)}(p^{l(q)q^{r(q)}}(m-1) + \cdots + 1),
\]
and since $q \mid m$ and $p^{l(q)} = 1(q)$, $q \mid (p^{l(q)q^{r(q)}}(m-1) + \cdots + 1)$; hence the $q$-Sylow subgroup of $E^*$ has only $q^{\alpha(r(q))}$ elements, so we have a contradiction. Thus $k^*$ is not $q$-divisible. QED

The following lemma is due to Van der Waerden (see [1, p. 58]).

Lemma. Let $a$, $r$ be integers $> 0$ and $a$ an integer $> 1$. Let $q$ be a prime number and
\[ T = \frac{(a^q - 1)}{(a^{q-1} - 1)}. \]

If a prime \( p \) divides \( T \) and \( a^{q-1} - 1 \), then \( q = p \). If \( q \) divides \( T \), then \( q \) divides \( a^{q-1} - 1 \). Finally, if \( q > 2 \) or \( r > 1 \), then \( T \neq 0(q^2) \).

**Proof.** We have

\[ T = \frac{(a^{q-1} - 1)q^{-1} + q(a^{q-1} - 1)q^{-2} + \cdots + q}{}. \]

This proves all the statements except when \( q = 2 \), and in that case, \( T = (a^{q-1} - 1) + 2 \), so that these assertions are also obvious. QED

**Definition.** We define the function \( \beta(q) \) for all primes \( q \neq p \) as follows:

\[ \begin{align*}
    p^{l(q)} - 1 &= q^{\beta(q)}l_q, & q \nmid l_q, q \neq 2, \\
    p^2 - 1 &= 2^{\beta(2)}l_2, & l_2 \text{ odd, } q = 2.
\end{align*} \]

**Proposition 4.** Let \( q \) be a prime such that \( G_q \) is finite and nontrivial. Then

\[ s(q) = \beta(q) + r(q) \quad \text{if } q \neq 2, \]
\[ s(2) = \beta(2) + r(2) - 1 \quad \text{if } q = 2, \text{ } p \neq 2, \]

where \( r \) and \( s \) are defined in equations (1) and (2) respectively.

**Proof.** Recall that the order of \( G_q \) is \( q^{l(q)} \). We are assuming \( G_q \) is finite and nontrivial, so \( F \) has an \( l(q) \)-extension in \( k \), and its maximal \( q \)-extension in \( k \) is finite. We also saw in the proof of Proposition 3 that the order of \( G_q \) is \( q^{\alpha(r(q))} \), where \( \alpha \) is defined in equation (4). Then by looking at the definitions of \( \alpha \) and \( \beta \), and by successively applying the lemma, where we let \( a = p^{l(q)} \), we see that (recalling \( l(2) = 1 \))

\[ \begin{align*}
    \alpha(r(q)) &= \beta(q) + r(q), & q \neq 2, \\
    \alpha(r(2)) &= \beta(2) + r(2) - 1. & QED
\end{align*} \]

**Theorem.** \( G(k/F) \) completely determines \( k^* \) in the sense of the supernatural number \( N \) explicitly determining the supernatural number \( M \).

**Proof.** Given any \( q \), if \( q = p \), \( G_p \approx (0) \) by Proposition 1, so \( s(p) = 0 \). If \( l(q) \nmid N \), \( G_q \approx (0) \) by Proposition 2, so \( s(q) = 0 \). If \( l(q) \mid N \) and \( r(q) = \infty \), \( G_q \approx Z(q^\infty) \) by Proposition 3, so \( s(q) = \infty \). If \( l(q) \mid N \) and \( r(q) < \infty \), \( G_q \) is finite, nontrivial and, by Proposition 4, \( s(q) = \beta(q) + r(q) \) if \( q \neq 2 \), \( s(2) = \beta(2) + r(2) - 1 \). QED

**Bibliography**


**Brown University**